SISTEM PENGAMANAN DAN PELAPORAN INTRUSI DARI SERANGAN WEB SERVER MENGGUNAKAN MODSECURITY

SKRIPSI

Disusun Oleh :

Aditya Noor Sandy
1034010079

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN"
JAWA TIMUR

2014

LEMBAR PENGESAHAN

SISTEM PENGAMANAN DAN PELAPORAN INTRUSI DARI SERANGAN WEB SERVER MENGGUNAKAN MODSECURITY

Disusun oleh :

ADITYA NOOR SANDY
1034010079

Telah disetujui mengikuti Ujian Negara Lisan
Gelombang II Tahun Akademik 2014 / 2015

Pembimbing I	Pembimbing II
Henni Endah W., S.T, M.Kom	I Made Suartana, S.Kom, M.Kom
NPT. 376091303481	NIP. 196111101991032001

Mengetahui,
Ketua Program Studi Teknik Informatika
Fakultas Teknologi Industri
Universitas Pembangunan Nasional ”Veteran” Jawa Timur

Budi Nugroho S.Kom, M.Kom
NPT. 3 8009 050 205 1

SKRIPSI

SISTEM PENGAMANAN DAN PELAPORAN INTRUSI DARI SERANGAN WEB SERVER MENGGUNAKAN MODSECURITY

Disusun Oleh :

ADITYA NOOR SANDY
1034010079

Telah dipertahankan dan diterima oleh Tim Penguji Skripsi
Program Studi Teknik Informatika Fakultas Teknologi Industri
Universitas Pembangunan Nasional "Veteran" Jawa Timur
Pada Tanggal 23 Desember 2014

Pembimbing :
1.

Henni Endah W., S.T, M.Kom.
NPT. 3 7609 13 0348 1

2.

I Made Suartana, S.Kom, M.Kom.
NIP. 196111101991032001

Tim Penguji :
1.

Wahyu Syaifullah JS., S.Kom, M.Kom
NPT. 3 8610 10 0296 1

2.

Henni Endah W., S.T, M.Kom.
NPT. 3 7609 13 0348 1

3.

I Gede Susrama, S.T, M.Kom.
NIP. 3 7006 06 0211 1

Mengetahui,
Dekan Fakultas Teknologi Industri
Universitas Pembangunan Nasional "Veteran" Jawa Timur

Ir. Sutiyono, MT.
NIP. 19600713 198703 1001

YAYASAN KESEJAHTERAAN PENDIDIKAN DAN PERUMAHAN
UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN" JAWA TIMUR
FAKULTAS TEKNOLOGI INDUSTRI

KETERANGAN REVISI

Kami yang bertanda tangan di bawah ini menyatakan bahwa mahasiswa berikut :

Nama : ADITYA NOOR SANDY
NPM : 1034010079
Jurusan : Teknik Informatika

Telah mengerjakan revisi / ~~tidak ada revisi~~*) pra rencana (design) / skripsi ujian lisan gelombang II , TA 2014/2015 dengan judul:

"SISTEM PENGAMANAN DAN PELAPORAN INTRUSI DARI SERANGAN WEB SERVER MENGGUNAKAN MODSECURITY"

Surabaya, 2 Januari 2015
Dosen Penguji yang memeriksa revisi

1) Wahyu Syaifullah JS., S.Kom, M.Kom. { }
NPT. 3 8608 10 0295 1

2) Henni Endah W., S.T, M.Kom. { }
NPT. 3 7809 13 0348 1

3) I Gede Susrama, S.T, M.Kom. { }
NIP. 3 7006 06 0211 1

Mengetahui,
Dosen Pembimbing

Pembimbing I	Pembimbing II
Henni Endah W., S.T, M.Kom	I Made Suartana, S.Kom, M.Kom.
NPT. 37809 13 0348 1	NIP. 11 3111 984

Judul	: SISTEM PENGAMANAN DAN PELAPORAN INTRUSI DARI SERANGAN WEB SERVER MENGGUNAKAN MODSECURITY
Pembimbing I	: Henni Endah W., S.Kom, M.Kom
Pembimbing II	: I Made Suartana, S.Kom, M.Kom
Penyusun	: Aditya Noor Sandy

ABSTRAK

Perkembangan jaringan berbasis web sekarang ini, banyak jenis sumber daya dan layanan yang disediakan oleh internet popular saat ini, seperti e-shopping, transaksi bisnis dan industri game online. Namun, dengan kenyamanan dan fasilitas ini, semakin banyak bahaya yang mengintai dan memicu perkembangan serangan web semakin pesat.

Dalam penelitian ini diimplementasikan sebuah system yang dapat mengatasi meningkatkan keamanan web secara efektif dengan menggunakan Web Application Firewall (WAF) yang berbasis aplikasi dalam bentuk modul web server dengan menggunakan metode rule base detection untuk mengatasi jenis serangan Sql Injection dan XSS terhadap web server serta mengimplementasikan sistem pelaporan intrusi menggunakan Jwall Auditconsole.

Dalam 10 kali uji coba serangan menggunakan 4 teknik serangan dengan dua scenario tanpa Waf dan menggunakan Waf didapatkan hasil yang menunjukan system dapat menangkal semua uji coba serangan dan mengenali serta melaporkan serangan dengan benar. Dengan ini didapatkan kesimpulan, sistem dapat meningkatan keamanan web dengan menangkal intrusi Sql Injection Dan XSS serta memberikan alert serangan kepada administrator web sehingga terbentuk interaksi yang baik antara system keamanan web dengan web administrator.

Kata Kunci : Web Application Firewall, Serangan Web, Modsecurity

KATA PENGANTAR

Dengan memanjatkan puji dan syukur atas Kehadirat Allah SWT atas segala rahmat, taufiq, serta Hidayah-Nya sehingga penyusun dapat menyelesaikan tugas akhir ini.

Tugas ini untuk memenuhi persyaratan untuk menempuh ujian sarjana pada Fakultas Teknologi Industri Program Studi Sistem Informasi Universitas Pembangunan Nasional "Veteran" Jawa Timur. Laporan ini disusun berdasarkan data – data yang diperoleh dan analisa yang dilakukan dengan judul "Sistem Pengamanan dan Pelaporan Intrusi dari Serangan Web Server Menggunakan Modsecurity"

Dengan selesainya Tugas Akhir ini, tak lupa penyusun mengucapkan terima kasih yang sebesar – besarnya, pada :

1. Allah SWT, Terimakasih atas Rahmat dan HidayahNya
2. Ibu dan Bapak saya yang telah banyak memberikan dukungan moril dan materiil.
3. Bpk. Budi Nugroho, S.Kom, M.Kom. selaku Ketua Program Studi Sistem Informasi FTI Universitas Pembangunan Nasional "Veteran" Jawa Timur, saya ucapkan terimakasih atas izin dan segala akses kemudahan yang diberikan selama pengerjaan tugas akhir berlangsung.
4. Bapak I Made Suartana, S.Kom, M.Kom dan Ibu Henni Endah W., S.T, M.Kom Selaku dosen pembibing yang selalu mendampingi saya, memberi ilmu dan arahan serta banyak membantu saya selama pengerjaan tugas akhir ini. Mohon maaf apabila ada tindakan maupun perkataan saya yang kurang berkenan di hati bapak dan Ibu. terimakasih banyak atas saran, nasehat, dan ilmu yang sudah diberikan kepada saya, semoga bermanfaat dimasa mendatang.
5. Seluruh dosen dan staf jurusan Teknik Informatika Universitas Pembangunan Nasional "Veteran" Jawa Timur yang telah banyak memberi ilmu, dukungan, bantuan, serta pengalaman yang akan sangat berguna bagi masa depan saya.
6. Bapak Ir. Sutiyono, MT selaku dekan Fakultas Teknologi Industri

7. Teman-teman Mahasiswa Teknik Informatika, sahabat - sahabat saya Heru, Affan, dan sahabat kost seperjuangan yang turut memberi masukkan dan dukungan, Suwun rek!!.
8. Dan semua pihak yang tidak dapat saya sebutkan satu persatu yang telah membantu dalam penyusunan sampai terselesaikannya tugas akhir ini.

Penyusun menyadari bahwa tugas akhir ini masih banyak kekurangan, oleh karena itu saran dan kritik yang membangun akan penyusun terima dengan lapang dada. Akhir kata semoga laporan ini dapat memberikan manfaat bagi semua pihak yang berkepentingan dan Allah SWT memberikan balasan kepada semua pihak yang telah memberikan bantuan.

Surabaya, 15 Desember 2014

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I

PENDAHULUAN

1.1 Latar Belakang

Dalam generasi jaringan berbasis web sekarang ini, banyak jenis sumber daya dan layanan yang disediakan oleh internet popular saat ini, seperti e-shopping, transaksi bisnis dan industri game online. Namun, dengan kenyamanan dan fasilitas ini, semakin banyak bahaya yang mengintai. Misalnya, cyber-crime yang sering terjadi pada game on-line, informasi pelanggan dari bank local yang bocor dan perampokan cyberbank yang terjadi pada salah satu bank dalam negeri. Oleh karena itu, berbagai perusahaan pengembang telah mengerahkan berbagai jenis fasilitas keamanan jaringan seperti Honeypot, Intrusion Detection System (IDS), dan Firewall.

Perkembangan jaringan berbasis web sekarang ini, berbagai perusahaan penyedia layanan jaringan telah menawarkan banyak layanan web seperti Penyimpanan halaman web, album web, blog. Setiap orang dapat memasukan request Http pribadi ke manapun seseorang terhubung ke Internet. Hal ini membuka kesempatan terhadap hacker dan cracker untuk menjalankan aksinya Namun disisi lain, kemampuan Intrusion Detection Sistem untuk

mendeteksi berbagai kegiatan serangan web yang bersifat fleksibel sangat terbatas .Sebagai contoh, banyak email spread dijaring berasal dari CNN pada bulan Agustus 2008, terdapat banyak situs Phishing beredar, dan Flash Malware BOTNET(Gartner Report, 2010). Selain itu, perkembangan serangan web semakin pesat, menurut laporan OWASP top 10 web attack dalam rentang waktu 2012 hingga 2013 serangan web tertinggi yang terjadi adalah Sql Injection dan XSS(OWASP, 2013), Hal ini mendorong peningkatan kebutuhan akan keamanan web server terhadap serangan tersebut.

Dalam tradisi perkembangan IDS saat ini masih sering menggunakan Regular Expressions untuk pencocokan pola serangan yang menjadikan hal ini tidak efisien dan tidak berguna ketika diserang oleh serangan web yang terbaru dan lebih fleksibel. Dalam hal ini dibutuhkan sebuah system yang dapat mengatasi masalah ini secara efektif, salah satunya adalah web application firewall (WAF) yang berbasis aplikasi dalam bentuk modul web server dengan menggunakan metode rule base detection. hal ini lebih fleksibel dari pada metode pencocokan pola (signature base), kerena metode serangan Web baru-baru ini biasanya menggunakan serangan multi-level atau multi-decoded yang selalu berubah ubah untuk menghindari serangan terdeteksi oleh IDS .

Tujuan dari tugas akhir ini adalah membuat sistem pengamanan dan pelaporan dengan menggunakan Waf Modsecurity dan tools audit console Jwall yang dibuat khusus untuk menampilkan dan mengkaji isi dari log file Modsecurity. Intrusi yang di cegah dari system ini adalah serangan Sql Injection dan Cross Site Scripting (XSS).

Manfaat dari Sistem yang akan di implementasikan ini adalah untuk menjaga validitas dan integritas data pada web server serta menjamin ketersediaan layanan bagi penggunanya dan melindungi web server dari serangan Sql Injection dan XSS serta, memudahkan administrator untuk mengontrol dan memantau keamanan web server secara langsung tanpa harus mengawasi langsung dari computer host/ server.

1.2 Rumusan Masalah

Sistem deteksi penyusupan jaringan yang ada saat ini umumnya mampu mendeteksi berbagai jenis serangan tetapi tidak mampu mengambil tindakan lebih lanjut. Selain itu sistem yang ada pada saat ini tidak memiliki interaktivitas dengan administrator pada saat administrator tidak sedang mengawasi sistemnya. Hal ini merupakan suatu hal yang tidak efektif terutama pada saat sistem berada dalam kondisi kritis. beberapa rumusan permasalahan yang ada dalam membangun sistem ini yaitu:

a. Bagaimana mengimplementasikan web application firewall Modsecurity untuk meningkatkan keamanan web terhadap serangan Sql Injection dan XSS.
b. Bagaimana mengolah log file menggunakan Audit Console guna memisahkan isi dari log file Modsecuriy.
c. Bagaimana mengiplementasikan website laporan serangan Jwall Audit Console yang terintergrasi dengan log Modsecurity.

1.3 Batasan Masalah

Pada penyelesaian tugas akhir ini terdapat beberapa batasan masalah yang dikaitkan dengan pembuatan pelaporan intrusi pada web server ini, antara lain :

a. Operating system yang digunakan adalah Ubuntu 12.04 64-bit.
b. Tool web application firewall adalah Modsecurity.
c. Tool yang digunakan untuk mengolah log file adalah Jwall audit console.
d. Intrusi yang difilter adalah XSS (Cros Site Scripting) dan Sql Injection.

1.4 Tujuan

Pada tugas akhir ini diimplementasikan system pengamanan dan pelaporan intrusi dari serangan web server. Adapun tujuan dari tugas akhir ini adalah :

a. Mendeteksi dan mencegah terjadinya intrusi terhadap Website dari serangan Sql Injection dan XSS.
b. Mengimplementasikan Website laporan untuk melaporkan aktifitas log serangan Sql Injection dan XSS (cross side scripting) yang terjadi pada Web server.

1.5 Manfaat

Keamanan Web server sebagai bagian dari sebuah sistem informasi adalah sangat penting untuk menjaga validitas dan integritas data serta menjamin ketersediaan layanan bagi penggunanya.maka dari itu, Sistem harus dilindungi dari segala macam serangan dan usaha-usaha penyusupan atau pemindaian oleh pihak yang tidak berhak. Sistem deteksi penyusupan jaringan yang ada saat ini umumnya mampu mendeteksi berbagai jenis serangan tetapi tidak mampu

mengambil tindakan lebih lanjut.beberapa manfaat dari tugas akhir ini adalah sebagai berikut :

a. Meningkatkan keamanan Website

   Membuat Website dengan tingkat keamanan yang tinggi sehingga tidak mudah untuk dirusak atau dimasuki oleh pihak – pihak yang tidak bertanggung jawab.

b. Terhindar dari Phising

   Website bebas dari ulah perusak tampilan dan peniru tampilan website yang telah dibangun, bahkan menghapus data penting yang ada di dalam database.

c. Memudahkan administrator

   Dengan adanya sistem ini administrator dapat mengawasi website yang di kelolanya dengan lebih fleksibel karena dalam sistem ini diinplementasikan website laporan serangan yang bisa diakses kapanpun.

1.6 Sistematika Penulisan

Sistematika penulisan tugas akhir ini akan membantu memberikan informasi tentang tugas akhir yang dijalankan dan agar penulisan laporan ini tidak menyimpang dari batasan masalah yang ada, sehingga susunan laporan ini sesuai dengan apa yang diharapkan. Sistematika penulisan laporan tugas akhir ini adalah sebagai berikut.

Bab I Pendahuluan

Bab ini berisi mengenai gambaran umum penelitian tentang latar belakang masalah, perumusan masalah, batasan masalah, tujuan tugas akhir, manfaat tugas akhir, dan sistematika penulisan.

Bab II Tinjauan Pustaka

Tinjauan pustaka berisi tentang berbagai konsep dasar penyerangan, tool pendukung, Web Aplication Firewall serta analisa yang digunakan dan teori-teori yang berkaitan dengan topik masalah yang diambil dan hal-hal yang berguna dalam proses analisis permasalahan.

Bab III Metode Penelitian

Metode tugas akhir ini berisi tentang rancangan jaringan, rancangan serangan-serangan, rancangan sistem klasifikasi, dan konfigurasi-konfigurasi yang digunakan dalam mendeteksi, serta metode-metode lain yang digunakan untuk menyelesaikan tugas akhir ini.

Bab IV Hasil dan Pembahasan

Dalam implementasi sistem ini berisi tentang hasil dan pembahasan tentang beberapa konfigurasi yang dilakukan pada bab sebelumnya untuk mengimplementasikan mesin sistem deteksi intrusi dengan Snort menggunakan Modsecurity core rule untuk meningkatkan efektifitas pendeteksian serangan web Sql Injection dan Cros Site

Scripting serta melakukan serangkaian uji coba untuk menganalisa kinerja sistem yang telah dibuat.

Bab V Kesimpulan Dan Saran

Berisi kesimpulan dan saran dari penulis yang sudah diperoleh dari hasil penulisan tugas akhir.